

Amendments to the Specification:

Please replace the paragraph [0001] with the following rewritten paragraph [00001]:

[0001] This application is a Continuation-In-Part of the following co-pending United States Patent Applications: ~~in the name of the inventors hereof (and others) and bearing the serial numbers, filing dates and titles shown below.~~

Serial No.	Filing Date	Title
10/243,858	September 13, 2002	System for Digital Content Access Control
10/243,355	September 13, 2002	Accessing for Digital Content Access Control
10/243,218	September 13, 2002	Synchronizing for Digital Content Access Control
10/243,474	September 13, 2002	Repositing for Digital Content Access Control
10/243,287	September 13, 2002	Provisioning for Digital Content Access Control

U.S. Patent Application Serial No. 10/243,858, entitled "System for Digital Content Access Control," of Jon Bostrom, Eduard K. de Jong and Aaron Cooley filed on September 13, 2002;

U.S. Patent Application Serial No. 10/243,355, entitled "Accessing for Digital Content Access Control," of Eduard K. de Jong, Aaron Cooley and Jon Bostrom, filed on September 13, 2002;

U.S. Patent Application Serial No. 10/243,218, entitled "Synchronizing for Digital Content Access Control," of Eduard K. de Jong filed on September 13, 2002;

U.S. Patent Application Serial No. 10/243,474, entitled "Repositing for Digital Content Access Control," of Eduard K. de Jong, Aaron Cooley and Jon

Bostrom filed on September 13, 2002, now U.S. Patent No. 7,240,365 issued on July 3, 2007;

U.S. Patent Application Serial No. 11/717,740 filed on March 12, 2007 in the name of inventors Eduard de Jong, Aaron Cooley and Jon Bostrom, entitled "Repositing for Digital Content Access Control", commonly assigned herewith and which is a continuation of U.S. Patent Application Serial No. 10/243,474; and

U.S. Patent Application Serial No. 10/243,287, entitled "Provisioning for Digital Content Access Control," of Eduard K. de Jong, Aaron Cooley and Jon Bostrom filed on September 13, 2002.

Please replace the paragraph [0002] with the following rewritten paragraph [00002]:

[0002] This application is related to the following:

U.S. Patent Application Serial No. 10/014,893, filed October 29, 2001 in the name of inventors Eduard de Jong, Moshe Levy and Albert Leung, entitled "User Access Control to Distributed Resources on a Data Communications Network", ~~Attorney Docket No. SUN-P6992,~~ commonly assigned herewith[.];

U.S. Patent Application Serial No. 10/040,270, filed October 29, 2001, in the name of inventors Eduard K. de Jong, Moshe Levy and Albert Leung, entitled "Enhanced Privacy Protection in Identification in a Data Communications Network", now U.S. Patent No. 7,085,840, issued August 1, 2006,~~Attorney Docket No. SUN-P6990,~~ commonly assigned herewith[.];

U.S. Patent Application Serial No. 10/014,823, filed October 29, 2001, in the name of inventors Eduard K. de Jong, Moshe Levy and Albert Leung, entitled "Enhanced Quality of Identification in a Data Communications Network", now U.S. Patent No. 7,085,840,

issued August 1, 2006, ~~Attorney Docket No. SUN P6991,~~
commonly assigned herewith[[]];

U.S. Patent Application Serial No. 10/014,934,
filed October 29, 2001 in the name of inventors Eduard
de Jong, Albert Y. Leung, and Moshe Levy, entitled
"Portability and Privacy with Data Communications
Network Browsing", ~~Attorney Docket No. SUN P7007,~~
commonly assigned herewith[[]];

U.S. Patent Application Serial No. 10/033,373,
filed October 29, 2001 in the name of inventors Eduard
de Jong, Albert Y. Leung, and Moshe Levy, entitled
"Managing Identification in a Data Communications
Network", ~~Attorney Docket No. SUN P7014,~~ commonly
assigned herewith[[]];

U.S. Patent Application Serial No. 10/040,293,
filed October 29, 2001 in the name of inventors Eduard
de Jong, Albert Y. Leung, and Moshe Levy, entitled
"Privacy and Identification in a Data Communications
Network", ~~Attorney Docket No. SUN P7015,~~ commonly
assigned herewith[[]];

U.S. Patent Application Serial No. 10/669,160,
filed September 2522, 2003, in the name of inventor
Eduard K. de Jong, entitled "Controlled Delivery of
Digital Content in a System for Digital Content Access
Control", ~~Attorney Docket No. SUN P8727,~~ commonly
assigned herewith[[]];

U.S. Patent Application Serial No. 10/668,687,
filed September 2522, 2003 in the name of inventor
Eduard K. de Jong, entitled "Accessing for Controlled
Delivery of Digital Content in a System for Digital
Content Access Control", ~~Attorney Docket No. SUN-~~
~~040105,~~ commonly assigned herewith[[]];

U.S. Patent Application Serial No. 10/687,217,
filed October 15, 2003 in the name of inventor Eduard
K. de Jong, entitled "Accessing In A Rights Locker
System for Digital Content Access Control", ~~Attorney~~
~~Docket No. SUN 040202,~~ commonly assigned herewith[[]];

U.S. Patent Application Serial No. 10/687,488,
filed October 15, 2003 in the name of inventor Eduard
K. de Jong, entitled "Rights Maintenance in a Rights
Locker System for Digital Content Access Control",
~~Attorney Docket No. SUN 040204~~, commonly assigned
herewith[[]]; and

U.S. Patent Application Serial No. 10/687,459,
filed October 15, 2003 in the name of inventor Eduard
K. de Jong, entitled "Embedded Content Requests in a
Rights Locker System for Digital Content Access
Control", ~~Attorney Docket No. SUN 040203~~, commonly
assigned herewith.

Please replace [0005] paragraph, with the following
rewritten paragraph [0005]:

[0005] A user desiring access to digital content 155-
170 stored by a digital content producer 105-120 uses a
mobile phone 125-140 to issue an access request to a
particular digital content producer 105-120. The
digital content producer 105-120~~195~~ authenticates the
user making the request. The authentication typically
includes prompting the user for a username and a
password if the username and password is not included
with the initial access request. Upon successful user
authentication, the digital content producer 105-120
may grant access to the digital content 155-170.
Alternatively, the digital content producer 105-120 may
issue a token that may be presented at a later time and
redeemed in exchange for access to the digital content.

Please replace paragraph [0016] with the following
rewritten paragraph [0016]:

[0016] In the context of the present invention, the
term "network" includes local area networks, wide area
networks, the Internet, cable television systems,

telephone systems, wireless telecommunications systems, fiber optic networks, Asynchronous Transfer Mode (ATM) networks, frame relay networks, satellite communications systems, and the like. Such networks are well known in the art and consequently are not further described here.

Please replace paragraph [0021] with the following rewritten paragraph [0021]:

[0021] In the context of the present invention, the term "cryptographic one-way function" describes any cryptographic process that produces an output based upon an input, such that it is computationally infeasible to compute the input based upon the output.

Exemplary cryptographic one-way functions comprise the Message-Digest algorithm 4 (MD4 algorithm) and the MD5 algorithm. The MD4 algorithm is described in R. Rivest, *The MD4 Message Digest Algorithm*, Request for Comments (RFC) 1320, MIT Laboratory for Computer Science and RSA Data Security, Inc., April 1992. The Message-Digest algorithm 5 (MD5 algorithm) is described in Rivest. R. *The MD5 Message-Digest Algorithm*, Request for Comments (RFC) 1321, MIT Laboratory for Computer Science and RSA Data Security, Inc., April 1992.

Please replace paragraph [0023] with the following rewritten paragraph [0023]:

[0023] In the context of the present invention, the term "Web page" describes a block of data available on a data communications network such as the World-Wide Web (WWW), identified by a Universal Resource Locator (URL). A Web page may comprise a file written in Hypertext Markup Language (HTML) and stored on a Web server. A Web page may also refer to one or more

images which appear as part of the page when it is displayed by a Web browser. The server may also generate one or more Web pages dynamically in response to a request, e.g. using a Common Gateway Interface (CGI) script. An HTML Web page may include one or more hypertext links ("clickable links") that refer to one or more other Web pages or resources. A user viewing the Web page using a browser may access the one or more other Web pages or resources by clicking on or otherwise activating the corresponding hypertext link.

Please replace paragraph [0026] with the following rewritten paragraph [0026]:

[0026] In the context of the present invention, the term "HyperText Transfer Protocol (HTTP) Request" describes a Web browser-initiated request for information from a Web server.

Please replace paragraph [0066] with the following rewritten paragraph [0066]:

[0066] Turning now to FIG. 15, a block diagram that illustrates a system for digital content access control where a secure user device activates deactivated tokens issued by a content provisioner and uses the activated tokens to access digital content stored by a content repository in accordance with one embodiment of the present invention is presented. System 1500 comprises a content provisioner 1505, a content repository 1515, a user device 1565 and a synchronizer 1520 in communication via network 1560. Content provisioner 1505 comprises a token issuer 1535 and content repository 1515 comprises a token acceptor 1540. User device 1565 comprises storage for deactivated tokens (1570). User device 1565 also comprises a secure user device ~~1505~~1510 that comprises a co-issuer 1525. The

co-issuer 1525 comprises a secret 1530 for activating deactivated tokens.

Please replace paragraph [0067] with the following rewritten paragraph [0067]:

[0067] In operation, user device 1565 communicates with content provisioner 1505 to obtain one or more deactivated tokens and stores them in deactivated token storage 1570. The one or more deactivated tokens 1545 are tied to particular digital content. Co-issuer 1525 activates the one or more deactivated tokens 1545 based at least in part on secret 1530. Secure user device ~~1505~~1510 presents one or more activated tokens 1550 to content repository 1515 to receive access to the digital content associated with the one or more activated tokens 1550. Content repository 1515 presents synchronizer 1555 with accepted tokens 1555. The synchronizer 1520 may recycle the previously accepted tokens 1555 to make them available for future token allocations. Synchronizer 1520 may also facilitate payment for delivery of digital content and receive payment in return for the accepted tokens. Synchronizer 1520 presents tokens to be recycled 1575 to content provisioner 1505 for subsequent reuse.

Please replace paragraph [0068] with the following rewritten paragraph [0068]:

[0068] According to one embodiment of the present invention, user device 1565 comprises a mobile phone and secure user device ~~1505~~1510 comprises a SIM card or the like.

Please replace paragraph [0069] with the following rewritten paragraph [0069]:

[0069] According to one embodiment of the present invention, co-issuer 1525 activates one or more deactivated tokens 1545 upon receipt by secure user device ~~1505~~1510 and stores the activated tokens in secure user device ~~1505~~1510 until the activated tokens are redeemed for access to digital content associated with the tokens. According to another embodiment of the present invention, secure user device ~~1505~~1510 stores one or more deactivated tokens until access to digital content associated with the deactivated tokens is desired. At that point, co-issuer 1525 activates the deactivated tokens and presents the activated tokens 1550 to content repository 1515 for access to digital content associated with the activated tokens.

Please replace paragraph [0070] with the following rewritten paragraph [0070]:

[0070] Turning now to FIG. 16, a block diagram that illustrates a system for digital content access control where a secure user device activates deactivated tokens issued by a content provisioner and uses the activated tokens to access digital content stored by a content repository in accordance with one embodiment of the present invention is presented. Figure 16 is similar to FIG. 15 except that secure user device ~~1605~~1610 in FIG. 16 comprises deactivated token storage 1670. In operation, user device 1665 communicates with content provisioner 1605 to obtain one or more deactivated tokens and stores them in deactivated token storage 1670. The one or more deactivated tokens 1645 are tied to particular digital content. Co-issuer 1625 activates the one or more deactivated tokens 1645 based at least in part on secret 1630. Secure user device ~~1605~~1610 presents one or more activated tokens 1650 to content repository 1615 to receive access to the

digital content associated with the one or more activated tokens 1650. Content repository 1615 presents synchronizer 1620 with accepted tokens 1655. The synchronizer 1620 may recycle the previously accepted tokens 1655 to make them available for future token allocations. Synchronizer 1620 may also facilitate payment for delivery of digital content and receive payment in return for the accepted tokens. Synchronizer 1620 presents tokens to be recycled 1675 to content provisioner 1605 for subsequent reuse.